Parametrizations for Families of ECM-Friendly Curves

Alexandre Gélin, Thorsten Kleinjung, Arjen K. Lenstra

PARAMETRIZATIONS FOR FAMILIES OF ECM-FRIENDLY CURVES

ALEXANDRE GÉLIN, THORSTEN KLEINJUNG, AND ARJEN K. LENSTRA

Abstract. We provide a new family of elliptic curves that results in a one to two percent performance improvement of the elliptic curve integer factorization method. The speedup is confirmed by extensive tests for factors ranging from 15 to 63 bits.

1. Introduction

The elliptic curve method (ECM) for integer factorization was introduced by H.W. Lenstra in 1985 and published two years later in [9]. It is the asymptotically fastest method that has been published for finding relatively small factors of large composites. Although the number field sieve [8] is the most efficient general algorithm for integer factorization, there are two common use cases for ECM: it is widely used in attempts to find factors of large composites for which no information is available about the sizes of the prime factors (R. Propper found the largest ECM factor so far, a 274-bit factor of $7^{337}+1$) and it is used for the so-called *cofactoring* step of the number field sieve (where many relatively small composites have to be factored).

Given an odd composite integer N to be factored, ECM performs arithmetic operations on elliptic curves considered to be defined over the finite field $\mathbf{F}_p$ of cardinality p, for an unknown prime divisor p of N. It may find p if the cardinality of at least one of these curves over $\mathbf{F}_p$ is smooth. For this reason, curves are used that are known to have favorable smoothness properties, such as a large torsion group over $\mathbf{Q}$ or a cardinality that is divisible by a fixed factor. Constructions of ECM-friendly curves were published by Suyama [11] (with a slight improvement by Montgomery in [10, Section 10.3.2]), Atkin-Morain [1], and generalized by Bernstein *et al.* in [4].

Originally formulated in [9] using Weierstrass curves, until around 2008 implementations of ECM mostly used Montgomery's approach from [10]. With the introduction of Edwards curves [6], a number of follow-up papers by Bernstein *et al.* [3, 5] ultimately led to "$a=-1$ *twisted Edwards*" curves by Hisil *et al.* [7] with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$ as one of the current most efficient ways to implement ECM, as shown by Bernstein *et al.* in [4]. For these curves, Barbulescu *et al.* in [2] identify three families that all have the same larger smoothness probability and an even better fourth family. In [2] a parametrization is provided for one of the three equivalent families; the others are only illustrated by — a finite set of — small values found by enumeration. In particular a parametrization of the fourth and best family, which could lead to a better choice of curves for ECM, has so far not been published. By *parametrization* we mean that an elliptic curve along with a non-torsion point is determined as a function of some parameter: in this paper

the parameter may be a point on some other elliptic curve or a rational number, thus giving rise to *elliptic* and *rational* parametrizations.

After a brief history in Section 2 on the use of Edwards curves in ECM, we present in Section 3 parametrizations for all families from [2] that remained to be parameterized. In Section 4 we compare our new curves to the ones used so far, observing that the curves derived from a same parametrization have similar behavior and that the fourth and best family indeed seems to lead to the best performance known for ECM. The resulting speed up is modest but worthwhile: given how much computing time is invested in ECM, the resulting practical savings could be considerable.

2. Edwards curves and elliptic curve method

Twisted Edwards curves. Let $\mathbf{K}$ be a field of characteristic different from 2. Edwards curves are defined in [6] by equations of the form $x^2 + y^2 = 1 + dx^2y^2$, for $d \in \mathbf{K}$ with $d(d-1) \neq 0$. To enlarge the set of curves, the equation was generalized in [3] to twisted Edwards curves $ax^2 + y^2 = 1 + dx^2y^2$ for $a, d \in \mathbf{K}$ with $ad(a-d) \neq 0$. Because of the favorable properties of the arithmetic in the curve group (speed and no exception for doubling) twisted Edwards curves gained interest in applications.

Torsion group. For each curve, stage 1 of ECM attempts to compute a scalar multiple of some initial point on the curve, for a scalar equal to the product of all prime powers up to some bound and where the computation is done modulo N. If the order of the initial point happens to be smooth modulo at least one but not all prime factors of N, an inversion failure modulo N reveals a factor of N. Because the torsion group E_{tors} of the curve over $\mathbf{Q}$ injects in the curve modulo each prime that has good reduction, in ECM it helps to choose curves that have a large E_{tors}. The largest gain that can be obtained in this manner is modest, because according to Mazur's theorem E_{tors} is isomorphic to

$$\mathbf{Z}/n\mathbf{Z} \text{ with } 1 \leq n \leq 10 \text{ or } n = 12, \text{ or } \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2n\mathbf{Z} \text{ with } 1 \leq n \leq 4.$$

The two most profitable possibilities, $\mathbf{Z}/12\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$, are characterized for families of Edwards curves in [5, Section 6]. On the other hand, the fastest scalar multiplication is obtained in [7] for $a=-1$ twisted Edward curves; as shown in [5], however, this limits the possibilities for interesting torsion groups (i.e., with cardinality greater than four) to

$$\mathbf{Z}/6\mathbf{Z},\ \mathbf{Z}/8\mathbf{Z} \text{ or } \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z},$$

thereby in particular excluding the two most profitable ones. For ECM the issue was settled in [4] where $a=-1$ twisted Edwards curves were compared to curves with E_{tors} isomorphic to $\mathbf{Z}/12\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$: it was found that the disadvantage of the formers' smaller torsion groups is outweighed by their faster scalar multiplication.

Curves with on average higher torsion modulo p. Barbulescu *et al.* in [2] further develop $a = -1$ twisted Edwards curves with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. In [4] these are shown to be the curves $-x^2 + y^2 = 1 - e^4x^2y^2$ with $e \notin \{0, \pm 1\}$. Compared to generic e-values and averaging over the primes p of good reduction, [2] uses Galois properties to identify four families of e-values

with increased average exponent of the prime 2 in the torsion group of the curve modulo p: for families

$$(i) : e = g^2; \quad (ii) : e = \frac{g^2}{2}, \quad \text{and} \quad (iii) : e = \frac{2g^2 + 2g + 1}{2g + 1} \tag{2.1}$$

the average exponent of the prime 2 increases by $\frac{1}{6}$ from $\frac{14}{3}$ to $\frac{29}{6}$ and for family

$$(iv) : e = \frac{g - \frac{1}{g}}{2} \tag{2.2}$$

it increases by $\frac{2}{3}$ from $\frac{14}{3}$ to $\frac{16}{3}$.

As an example, although the cardinality of the torsion group over $\mathbf{Q}$ equals eight, it is shown in [2] that for the best case (family (iv)) the cardinality of the torsion group of the curve modulo p is divisible by 16, and by 32 if $p \equiv 1 \bmod 4$ and $g(g-1)(g+1)$ is a quadratic residue modulo p.

Usage of these curves in ECM requires an easy way to generate them, along with an appropriate initial point on each curve. Earlier and new ways to do this are discussed in the next section.

3. Parametrizations for curves with higher torsion modulo p

In this section we are exclusively interested in the generation of $a = -1$ twisted Edwards curves with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. The first known parametrization for the general case of such curves is the *elliptic parametrization* from [4, Theorem 3.3]; it generates a target curve (and a point of infinite order on it) as a function of a point on another elliptic curve of positive rank. Our goal is to find elliptic parametrizations for all four families (i)-(iv) in (2.1) and (2.2).

For family (i) this has already been done in [2]. First a new *rational parametrization* for the general case was derived, i.e., a function from $\mathbf{Q}$ — with finitely many exceptions — to $a = -1$ twisted Edwards curves with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, along with a point of infinite order on each curve. It was then checked if a special choice of the rational parameters leads to curves with e-values as in (2.1) or (2.2). That turned out to work for family (i), but due to limitations imposed by the rational parametrization it failed for families (ii)-(iv).

In this section we review the approach from [2], and we present the results of a search that we conducted for new rational parametrizations for the general case. The newly found rational parametrizations turn out to suffice for our purpose: following the approach from [2] it is shown that special choices of the rational parameters lead to elliptic parametrizations for all four families (i)-(iv).

General conditions. From the equation $-x^2 + y^2 = 1 - e^4x^2y^2$ with $e \notin \{0, \pm 1\}$ for the general case, it follows that e and $-e$ lead to the same curve. Considering the variable change $(x, y) \longmapsto (xe^2, \frac{1}{y})$, the curves for e and $\frac{1}{e}$ are birationally equivalent. Thus, only one element of $\{\pm e, \pm\frac{1}{e}\}$ is of interest and we fix $e > 1$.

Furthermore, as we require points of infinite order, the curves must have positive rank and easily identifiable torsion points in order to be able to avoid them. The latter can be done, because

- $(0, 1)$ is the neutral element,
- $(0, -1)$ and $\left(\infty, \pm\frac{1}{e^2}\right)$ are the three 2-torsion points, and
- $(\pm\frac{1}{e}, \pm\frac{1}{e})$ are the four 4-torsion points.

A point (x, y) on the curve is therefore a non-torsion point if and only if $x \notin \{0, \infty\}$ and $xe \neq \pm 1$.

Earlier parametrizations. As mentioned above, the first parametrization for the general case, from [4, Theorem 3.3], works by selecting a particular elliptic curve over $\mathbf{Q}$ of positive rank and by showing how a rational point on it provides an $a=-1$ twisted Edwards curve with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, along with a non-torsion point. The first rational parametrization generalizes this approach. It is [2, Theorem 3.7]:

Theorem 3.1. *For nonzero $t \in \mathbf{Q} \setminus \{\pm 1, \pm 3^{\pm 1}\}$ let*

$$e_1 = \frac{3(t^2-1)}{8t}, x_1 = \frac{1}{4e_1^3 + 3e_1} = \frac{128t^3}{27t^6 + 63t^4 - 63t^2 - 27} \text{ and } y_1 = \frac{9t^4 - 2t^2 + 9}{9t^4 - 9}.$$

Then (x_1, y_1) is a non-torsion point on the $a=-1$ twisted Edwards curve $-x^2+y^2 = 1 - e_1^4 x^2 y^2$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

Proof. The excluded t-values imply that $e \notin \{0, \pm 1\}$ and that x_1 and y_1 are well-defined. The point (x_1, y_1) can be seen to be on the curve and it is a non-torsion point because $x_1 \notin \{0, \infty\}$ and $x_1 e_1 \neq \pm 1$. □

Compared to the parametrization from [4, Theorem 3.3], the above rational parametrization reduces the computation required for curve generation, and the simple formula for e facilitates the search for t-values that lead to an e-value that satisfies (2.1) or (2.2). It is easy to check if a rational e-value belongs to family (i) or (ii). Families (iii) and (iv) look more cumbersome, but can easily be dealt with using the following alternative characterizations.

- Because $e = \frac{2g^2+2g+1}{2g+1}$ if and only if $2g^2 + 2(1-e)g + (1-e) = 0$ and because a rational g satisfying the latter polynomial exists if and only if the discriminant $4(e^2-1)$ is a rational square, it follows that
$$e = \frac{2g^2 + 2g + 1}{2g + 1} \iff e^2 - 1 \text{ is a square.}$$
- Arguing identically (which results in discriminant $4(e^2+1)$) it follows that
$$e = \frac{g - \frac{1}{g}}{2} \iff e^2 + 1 \text{ is a square.}$$

Corollary 3.2. *(This is* [2, Corollary 3.8]*.) Consider the elliptic curve $y^2 = x^3 - 36x$ of rank one, with the point $(-3, 9)$ generating a non-torsion subgroup. For any point (x, y) on this curve and*

$$t = \frac{x+6}{x-6}$$

the $a=-1$ twisted Edwards curve with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ defined as in Theorem 3.1 belongs to family (i) and has positive rank over $\mathbf{Q}$.

Proof. This follows from

$$e_1 = \frac{3(t^2-1)}{8t} = \frac{9x}{x^2 - 36} = \left(\frac{3x}{y}\right)^2$$

and the fact that (x_1, y_1) is a non-torsion point. □

Remark 3.3. Corollary 3.2 provides an elliptic parametrization for family (i). Attempting this approach for the other three families gives rise to curves of rank zero, and thus not the infinite families desired.

New rational parametrizations. To find new infinite families of curves, we rewrite the general case equation $-x^2 + y^2 = 1 - e^4x^2y^2$ as

$$y^2 = \frac{1+x^2}{1+e^4x^2}. \tag{3.1}$$

The resulting condition that the right hand side is a square is equivalent to requiring that $(1+x^2)(1+e^4x^2) = e^4x^4 + (1+e^4)x^2 + 1$ is a square. With $x = \frac{u}{v}$ we get the equivalent condition that for the chosen values of e, u, and v the polynomial $e^4u^4 + (1+e^4)u^2v^2 + v^4$ must evaluate to a square.

Choosing u and v as polynomials in e, we are interested in the square-free part of the resulting polynomial in e and in e-values for which the square-free part evaluates to a rational square. A square-free part of degree higher than four corresponds to a hyperelliptic curve that is known to have a finite number of rational points; because we are interested in infinite families of curves, this case is of no interest to us.

The following search was conducted (using PARI/GP [12] for the polynomial factorizations):

- $x = u^{\pm 1}$ for all integer polynomials u of degree at most two and coefficients absolutely bounded by 100, and of degree at most four and coefficients absolutely bounded by ten;
- $x = \frac{u}{v}$ for all integer polynomials u, v of degree at most three and coefficients absolutely bounded by ten.

The only square-free part of degree two thus found leads to the rational parametrization from Theorem 3.1. All other square-free parts have degree equal to four, and thus each corresponds to an elliptic curve. Each one that has positive rank then leads to an elliptic parametrization (i.e., curves as functions of points on some other elliptic curve), but as we set out to find rational parametrizations (i.e., curves as functions of rational numbers) this is not what we are interested in.

To address this we "manually" searched through the polynomials attempting to find commonalities among the relevant square-free parts, which ultimately resulted in parameterized infinite families of curves. Given such an infinite curve parametrization (parameterized by k in the example below), it suffices to parameterize a finite number of points per curve. Our approach essentially consists in identifying these families from the derived small values and check if they lead to good subfamilies.

Example 3.4. *To illustrate this strategy, substituting* $\frac{e+k}{ke-1}$ *for* x *in Equation* (3.1)*, it is found that* $\frac{k^2+1}{e^4+2ke^3+(k^2-1)e^2-2ke+1}$ *must be a square. With the fixed point* $e = \frac{3}{4k}$ *the denominator becomes* $(\frac{4k^2+9}{16k^2})^2$ *so that for each* k *for which* k^2+1 *is a square, we have a point* (x, y) *satisfying the curve equation* $-x^2 + y^2 = 1 - \left(\frac{3}{4k}\right)^4 x^2y^2$ *for the general case. This results in infinitely many such curves.*

Using several families of degree four polynomials (and, for some, different points on the same curve), this resulted in the six additional new rational parametrizations in Theorem (3.5), the proof of which is identical to the proof of Theorem 3.1. For completeness the earlier result from Theorem 3.1 is included.

Theorem 3.5. *For $1 \le j \le 7$ and for each nonzero $t \in \mathbf{Q} \setminus S_j$ the point (x_j, y_j) is a non-torsion point on the $a=-1$ twisted Edwards curve $-x^2 + y^2 = 1 - e_j^4 x^2 y^2$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$:*

j	S_j	e_j	x_j	y_j
1	$\{\pm 1, \pm 3^{\pm 1}\}$	$\frac{3(t^2-1)}{8t}$	$\frac{128t^3}{27t^6+63t^4-63t^2-27}$	$\frac{9t^4-2t^2+9}{9t^4-9}$
2	$\{-2, -1, \pm 4\}$	$\frac{t^2+2t+4}{2t+2}$	$\frac{2t^3+2t^2-8t-8}{t^4+6t^3+12t^2+16t}$	$\frac{2t^5+14t^4+40t^3+44t^2+32t+16}{t^6+4t^5+10t^4+20t^3+40t^2+64t+64}$
3	$\{\pm 2\}$	$\frac{t^2+4}{3t}$	$\frac{12t^2-24}{t^4-4t^2-32}$	$\frac{3t^6-12t^4+120t^2}{5t^6+12t^4+128}$
4	$\{-2, -1, \pm 4\}$	$\frac{t^2+4t}{t^2-4}$	$\frac{2t^3+2t^2-8t-8}{t^4+6t^3+12t^2+16t}$	$\frac{t^6+6t^5+10t^4-16t^3-48t^2-32t-32}{t^6+6t^5+10t^4+16t^3+48t^2+64t}$
5	$\{\pm 4, \pm 8\}$	$\frac{4t^4-1024}{t^5+512t}$	$\frac{96t^6+49152t^2}{t^8-1280t^4+262144}$	$\frac{t^{12}+3840t^8+1966080t^4+134217728}{t^{12}-768t^8+786432t^4-167772160}$
6	$\{\pm 1, \pm 2, \pm 4\}$	$\frac{t^3+8t}{4t^2+8}$	$\frac{12t^2+24}{t^4+4t^2-32}$	$\frac{4t^6+24t^4+192t^2+320}{5t^6+48t^4+96t^2+256}$
7	$\{\pm 2\}$	$\frac{t^3-8t}{4t^2-8}$	$\frac{12t^2-24}{t^4-4t^2-32}$	$\frac{4t^6-24t^4+192t^2-320}{5t^6-48t^4+96t^2-256}$

Imposing the aforementioned conditions to obtain all four families (i)-(iv) (as mentioned above, it suffices to test if $\{e, 2e, e^2 \pm 1\}$ contains a square) leads to the corollary below. For completeness it includes the result of Corollary 3.2.

Corollary 3.6. *For $1 \le j \le 4$ let (e_j, x_j, y_j) be functions of t as in Theorem 3.1. For each case below the elliptic curve E has rank one, torsion group consisting of the set T adjoined with the neutral element, and non-torsion point Q, and for each point (x, y) on E the pair (x_j, y_j) is a non-torsion point on the $a=-1$ twisted Edwards curve $-x^2+y^2 = 1-e_j^4 x^2 y^2$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$ of positive rank and of the family listed. The last two columns list the e_j-value of the first curve constructed along with the non-torsion point.*

family	j	E	T	Q	t	*curve generated by Q:* e_j	*non-torsion point*
(i)	1	$y^2 = x^3 - 36x$	$\{(0,0), (\pm 6, 0)\}$	$(-3, 9)$	$\frac{x+6}{x-6}$	$\frac{16}{9}$	$\left(\frac{12}{91}, \frac{27}{29}\right)$
(ii)	2	$y^2 = x^3 + 3x$	$\{(0,0)\}$	$(1, 2)$	$x - 1$	$\frac{49}{8}$	$\left(\frac{440}{1911}, \frac{15688}{132937}\right)$
(ii)	3	$y^2 = x^3 + 9x$	$\{(0,0)\}$	$(4, 10)$	$\frac{2x}{3}$	$\frac{25}{18}$	$\left(\frac{48}{575}, \frac{15579}{15725}\right)$
(iii)	3	$y^2 = x^3 - x^2 - 64x + 64$	$\{(1,0), (\pm 8, 0)\}$	$(-6, 14)$	$\frac{8x-8}{y}$	$\frac{5}{3}$	$\left(\frac{21}{20}, \frac{87}{185}\right)$
(iii)	4	$y^2 = x^3 - 12x$	$\{(0,0)\}$	$(-2, 4)$	$\frac{x-2}{2}$	$\frac{65}{56}$	$\left(\frac{252}{3965}, \frac{444976}{445705}\right)$
(iv)	4	$y^2 = x^3 - x^2 - 9x + 9$	$\{(1,0), (\pm 3, 0)\}$	$(5, 8)$	$\frac{4x+4}{y-4}$	$\frac{15}{8}$	$\left(\frac{28}{195}, \frac{3152}{3495}\right)$

Proof. With the proof of Corollary 3.2 and the characterizations given before it, the verifications in the table below suffice. □

family	j	
(ii)	2:	$e_2 = \frac{t^2+2t+4}{2t+2} = \frac{x^2+3}{2x} = \frac{1}{2}\left(\frac{y}{x}\right)^2$
(ii)	3:	$e_3 = \frac{t^2+4}{3t} = \frac{2x^2+18}{9x} = \frac{1}{2}\left(\frac{2y}{3x}\right)^2$
(iii)	3:	$e_3^2 - 1 = \frac{x^4-4x^3+132x^2-256x+4096}{36y^2} = \left(\frac{x^2-2x+64}{6y}\right)^2$
(iii)	4:	$e_4^2 - 1 = \frac{16x^3-192x}{x^4-8x^3-8x^2+96x+144} = \left(\frac{4y^2}{x^2-4x-12}\right)^2$
(iv)	4:	$e_4^2 + 1 = \left(\frac{x^4+4x^3+14x^2-108x+153}{x^4-4x^3-18x^2-16xy+12x+48y+9}\right)^2$

Remark 3.7. Two of the curves in the e_j-column of the table in Corollary 3.6 already appeared in [4, Table 3.1], namely those in the first and fourth row (though for the latter [4] used the different non-torsion point $\left(\frac{27}{11}, \frac{5}{13}\right)$).

The search that led to Corollary 3.6 did not identify any elliptic curve of positive rank for $j > 4$, and no other elliptic curve of positive rank for $j \leq 4$ either.

4. Effectiveness of the new curves

In this section we consider the effectiveness of our new curves when used in ECM and compare them to the curves proposed for ECM in [4]. To facilitate the comparison we conduct the same tests as in [4] and borrow some of their notation.

Earlier work. In [4] the effectiveness of Edwards curves for ECM was investigated. For each of the five torsion groups (isomorphic to $\mathbf{Z}/6\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/12\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$) a set of a thousand Edwards curves was generated as described in [4], with $a = -1$ when possible (i.e., for the three smallest torsion groups). For each of the 5000 resulting curves the EECM software from [5] was applied to all b-bit primes for $15 \leq b \leq 26$ (with ECM bounds depending on the targeted b-bit prime as in [5]). For each curve and each b the number of b-bit primes found (the "yield") was tallied, with the resulting counts extensively detailed in five very informative tables. Here a prime p is said to be "found" by a curve if the cardinality of the curve over $\mathbf{F}_p$ is smooth with respect to the ECM bounds used.

On average the curves with torsion group isomorphic to $\mathbf{Z}/6\mathbf{Z}$ performed best, because of the relatively large number of primes found and because $a = -1$ allows fast scalar multiplication. Among these, a particularly good curve is $-x^2 + y^2 = 1 - \frac{13312}{18225}x^2y^2$, identified by the non-torsion point $\left(\frac{825}{2752}, \frac{1521}{1504}\right)$ in the #1-column (for $b = 21$ and $b \geq 24$) and #2-column (for $b = 19, 22$) of [4, Table 5.1]. We re-derived its tallies for the $\mathcal{C}_6$-column of Table 1 (six figures of which thus already appeared in [4, Table 5.1]). Another interesting result was that among the curves with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ four curves appeared to stand out. Indeed, these four curves happened to belong to the families with favorable Galois properties that were identified in [2]: two of family (i) and one each of families (iii) and (iv) and in [4, Table 3.1] identified by the non-torsion points $\left(\frac{12}{91}, \frac{27}{29}\right)$, $\left(\frac{3}{14}, \frac{1}{17}\right)$, $\left(\frac{27}{11}, \frac{5}{13}\right)$, and $\left(\frac{12}{343}, \frac{1404}{1421}\right)$, respectively. The latter one "easily outperforms" the other 999 curves for $b \geq 19$, the reason of which is not identified in [2] and which we now know to be due to the fact that it is of family (iv)[1]: in [4, Table 3.1] it is "best" for $b = 17$ and $b \geq 19$ and "second best" for $b = 16, 18$. This curve has equation $-x^2 + y^2 = 1 - \left(\frac{77}{36}\right)^4 x^2y^2$ and does not appear in our parametrization of curves of family (iv). Its re-derived tallies are listed in the $\mathcal{C}_{2\times4}$-column of Table 1 (all figures of which except for $b = 15$ thus already appeared in the #1 or #2-column of [4, Table 3.1]).

Comparison to earlier work. For one hundred curves of family (iv) as parameterized in the last row of the table in Corollary 3.6 we ran the same tests as in [4] with the same EECM software and parameters. The curves we used are denoted by $\mathcal{C}_{[m]}$ for $1 \leq m \leq 100$, where $\mathcal{C}_{[m]}$ is constructed from the point $(x, y) = mQ$ with $Q = (5, 8)$ on the curve $y^2 = x^3 - x^2 - 9x + 9$. The #1 and #100-column in Table 1 list the largest and smallest, respectively, number of primes found per

[1]This was recognized by Peter L. Montgomery.

curve, with the average-column averaging the counts over all one hundred curves. Results of the tests for families (i)-(iii) are less interesting and not reported.

Per b-value the ratio of the best yield over $\mathcal{C}_{[1]}, \mathcal{C}_{[2]}, \ldots, \mathcal{C}_{[100]}$ and the yield of the single best performing earlier curve $\mathcal{C}_6$ is given in the ${}^{\#1}/_{\mathcal{C}_6}$-column of Table 1, but no single new curve has been identified that actually realizes the small gain suggested (but see Table 2 below). Indeed, the outcome of the same performance comparison between the average of the $\mathcal{C}_{[m]}$-curves and $\mathcal{C}_6$ is more variable and with 65 of the one hundred $\mathcal{C}_{[m]}$-curves having a higher average yield than $\mathcal{C}_6$, the performance is close. The curve with the best average ratio (of 1.0064) compared to $\mathcal{C}_6$ is $\mathcal{C}_{[93]}$, and curves $\mathcal{C}_{[22]}$ and $\mathcal{C}_{[86]}$ are the only two curves that have higher yield than $\mathcal{C}_6$ (and thus than $\mathcal{C}_{2\times4}$) for all but three b-values; there are ten $\mathcal{C}_{[m]}$ curves for which the yield is lower than for $\mathcal{C}_6$ for four b-values. As can be seen in Table 1, for $b = 23$ all $\mathcal{C}_{[m]}$-curves considered have higher yield than $\mathcal{C}_6$. Unlike [4], we do not specify which of $\mathcal{C}_{[1]}, \mathcal{C}_{[2]}, \ldots, \mathcal{C}_{[100]}$ has the best yield because with no curve appearing more than twice among the "top three" this information is useless. This is illustrated, in the ${}^{\#1}/_{\#100}$-column, by the ratio of the yields of the best and worst performing $\mathcal{C}_{[m]}$ per b-value: with small ratios all $\mathcal{C}_{[m]}$-curves tested can be seen to behave similarly. The figures in the ratio-columns of the tables in [4] are much larger — with one thousand curves per table they not only cast their net much wider, but they also allow a greater variation (of Galois properties) of curves per batch.

TABLE 1. Yields for $\mathcal{C}_6$ and the family (iv) curves $\mathcal{C}_{2\times4}$, $\mathcal{C}_{[1]}, \mathcal{C}_{[2]}, \ldots, \mathcal{C}_{[100]}$.

b	$\mathcal{C}_6$	$\mathcal{C}_{2\times4}$	#1 (among $\mathcal{C}_{[1]}, \mathcal{C}_{[2]}, \ldots, \mathcal{C}_{[100]}$)	average	#100	${}^{\#1}/_{\mathcal{C}_6}$	${}^{\#1}/_{\#100}$
15	1127	1049	1202	1155.36	1103	1.0665	1.0897
16	1693	1564	1806	1737.32	1664	1.0667	1.0853
17	3299	2985	3324	3197.86	3077	1.0075	1.0802
18	6150	5529	6168	6020.01	5921	1.0029	1.0417
19	10802	10200	10881	10723.75	10500	1.0073	1.0362
20	16148	15486	16396	16197.71	15955	1.0153	1.0276
21	24160	22681	24312	24003.34	23655	1.0062	1.0277
22	48378	46150	48894	48515.60	48114	1.0106	1.0162
23	83339	82743	85525	84839.98	84254	1.0262	1.0150
24	193069	187596	193558	192825.73	191961	1.0025	1.0083
25	318865	311864	320498	319154.79	317304	1.0051	1.0100
26	493470	480006	495082	493556.42	492364	1.0032	1.0055

All our parameterized curves have higher yields than the curve $\mathcal{C}_{2\times4}$, even though they are all family (iv) curves. This is due to our choice of the non-torsion point (x_j, y_j) which implies that the group of the curve modulo about half of the primes contains a point P such that $(x_j, y_j) = 2P$, thereby for those primes effectively adding a doubling in the scalar multiplication in ECM. The effect diminishes with larger b-values (see also the last column of Table 2).

Additional tests. On the EECM website[2] the yields of ECM using a fixed Edwards curve are given when applied to batches of 2^{20} b-bit primes, for b up to 63. We used the same EECM software and parameters (but our own sets of 2^{20} b-bit primes) to conduct the same experiment for the following four Edwards curves:

- the curve $\mathcal{C}_{[1]} : -x^2+y^2 = 1-\left(\frac{15}{8}\right)^4 x^2y^2$, the first curve of our parametrization of family (iv) curves;
- the above curve $\mathcal{C}_6$, i.e., the best performing curve from [4];
- the curve $\mathcal{C}_{12} : x^2 + y^2 = 1 - \frac{24167}{25}x^2y^2$ from the EECM website, with torsion group of order twelve and a non-torsion point $\left(\frac{5}{23}, \frac{-1}{7}\right)$ with very small coordinates;
- the above curve $\mathcal{C}_{2\times 4}$ from [4] belonging to family (iv), but not appearing in our parametrization of family (iv) curves.

As can be seen in Table 2 the yields are very close. The average yield-ratios of curve $\mathcal{C}_{[1]}$ compared to the three other curves (in the last row of Table 2) suggest that the new curve $\mathcal{C}_{[1]}$ overall performs best. Note too that the three other curves were chosen as the best among large batches of previously known curves, whereas $\mathcal{C}_{[1]}$ is just the first one of our newly parameterized family (iv) curves. Based on the final column of Table 1, we expect that all these new curves behave similarly.

The non-monotone yield decrease, consistent among the four curves tested, can be attributed to the choice of parameters in the EECM software.

5. Conclusion

In [2] favorable properties of the Galois group structures of $a = -1$ twisted Edwards curves with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$ were identified. This gave rise to four families of curves that looked promising for application in ECM. A new rational parametrization of $a=-1$ twisted Edwards curves with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ then led to an elliptic parametrization for the curves in one family, but not the most promising one.

In this paper we extended the constructions from [2] by developing six further rational parametrizations, and use three of them to formulate five new elliptic parametrizations that enable fast generation of curves for all families of curves from [2]. We conducted the same tests as described in [4] for the family of curves that are, based on their Galois properties, most promising for ECM. With respect to the criteria from [4] usage of this family of curves leads to slightly better performance of ECM than reported before, with no significant fluctuations across curves from this same family. The newly parameterized curves may prove to be most useful for ECM-based cofactoring in the number field sieve. We do not claim that our results are complete: other parametrizations than the ones presented in this paper may exist.

All potential new savings identified in this paper rely on the properties of the curves used, not on the way arithmetic on the curve is performed. Indeed, we rely on the same improvement from [7] that is exploited in [4] and use the same software that was used in [4].

[2] `http://eecm.cr.yp.to/performance.html`

TABLE 2. Yield comparisons for $\mathcal{C}_{[1]}$ versus $\mathcal{C}_6$, $\mathcal{C}_{12}$ and $\mathcal{C}_{2\times4}$.

b	$\mathcal{C}_{[1]}$	$\mathcal{C}_6$	$\mathcal{C}_{[1]}/\mathcal{C}_6$	$\mathcal{C}_{12}$	$\mathcal{C}_{[1]}/\mathcal{C}_{12}$	$\mathcal{C}_{2\times4}$	$\mathcal{C}_{[1]}/\mathcal{C}_{2\times4}$
27	263563	260933	1.0100	257558	1.0233	259377	1.0161
28	212253	209813	1.0116	206965	1.0255	208819	1.0164
29	179190	176620	1.0145	174302	1.0280	176699	1.0140
30	141182	139827	1.0096	137953	1.0234	138984	1.0158
31	197013	195906	1.0056	193954	1.0157	195365	1.0084
32	161111	159685	1.0089	158323	1.0176	159552	1.0097
33	129949	128477	1.0114	127719	1.0174	128326	1.0126
34	131982	131397	1.0044	130116	1.0143	130511	1.0112
35	131837	130694	1.0087	129699	1.0164	131161	1.0051
36	114826	113772	1.0092	112689	1.0189	113775	1.0092
37	103744	102681	1.0103	102515	1.0119	103173	1.0055
38	85135	83839	1.0154	83778	1.0161	84120	1.0120
39	73526	73069	1.0062	72897	1.0086	73376	1.0020
40	59619	59265	1.0059	58970	1.0110	59955	0.9943
41	83967	83694	1.0032	83295	1.0080	83323	1.0077
42	73730	73739	0.9998	73653	1.0010	73249	1.0065
43	60978	60573	1.0066	60611	1.0060	60695	1.0046
44	50238	49714	1.0105	49509	1.0147	50077	1.0032
45	44354	43706	1.0148	43825	1.0120	44259	1.0021
46	40133	39754	1.0095	39385	1.0189	39873	1.0065
47	46291	46167	1.0026	45951	1.0073	46240	1.0011
48	40969	40569	1.0098	40683	1.0070	40703	1.0065
49	37956	37428	1.0141	37099	1.0231	37555	1.0106
50	35096	34963	1.0038	35421	0.9908	35202	0.9969
51	29503	29105	1.0136	29023	1.0165	29209	1.0100
52	29780	29191	1.0201	29342	1.0149	29666	1.0038
53	27430	27153	1.0102	27069	1.0133	27594	0.9940
54	23996	23667	1.0139	23896	1.0041	23649	1.0146
55	25316	25064	1.0100	24883	1.0174	25023	1.0117
56	22471	22255	1.0097	21828	1.0294	22411	1.0026
57	20449	20169	1.0138	20253	1.0096	20276	1.0085
58	20826	20313	1.0252	20303	1.0257	20578	1.0120
59	18527	18231	1.0162	18029	1.0276	18340	1.0101
60	16287	16016	1.0169	16021	1.0166	16306	0.9988
61	13638	13482	1.0115	13488	1.0111	13462	1.0130
62	18056	18083	0.9985	18071	0.9991	18351	0.9839
63	15657	15651	1.0003	15613	1.0028	15747	0.9942
	averages		$\mathcal{C}_{[1]}/\mathcal{C}_6$: 1.0099		$\mathcal{C}_{[1]}/\mathcal{C}_{12}$: 1.0142		$\mathcal{C}_{[1]}/\mathcal{C}_{2\times4}$: 1.0063

ACKNOWLEDGEMENTS

This work has been supported in part by the European Union's H2020 Programme under grant agreement number ERC-669891.

References

1. Arthur O. L. Atkin and François Morain, *Finding suitable curves for the elliptic curve method of factorization*, Mathematics of Computation **60** (1993), 399–405.
2. Razvan Barbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery, *Finding ECM-friendly curves through a study of Galois properties*, Proceedings of the Tenth Algorithmic Number Theory Symposium, 2012, pp. 63–86.
3. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted Edwards curves*, Progress in Cryptology - AFRICACRYPT 2008, Proceedings, 2008, pp. 389–405.
4. Daniel J. Bernstein, Peter Birkner, and Tanja Lange, *Starfish on strike*, Progress in Cryptology - LATINCRYPT 2010, Proceedings, 2010, pp. 61–80.
5. Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *ECM using Edwards curves*, Mathematics of Computation **82** (2013), no. 282, 1139–1179.
6. Harold M. Edwards, *A normal form for elliptic curves*, Bulletin of the American Mathematical Society **44** (2007), 393–422.
7. Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson, *Twisted Edwards curves revisited*, Advances in Cryptology - ASIACRYPT 2008, Proceedings, 2008, pp. 326–343.
8. Arjen K. Lenstra and Hendrik W. Lenstra Jr., *The development of the number field sieve*, Lecture Notes in Mathematics, vol. 1554, Springer-Verlag, 1993.
9. Hendrik W. Lenstra Jr., *Factoring integers with elliptic curves*, Annals of Mathematics **126** (1987), 649–673.
10. Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of Computation **48** (1987), 243–264.
11. Hiromi Suyama, *Informal preliminary report*, (cited in [10]), 1985.
12. The PARI Group, Bordeaux, *PARI/GP version* `2.7.0`, 2014, available from `http://pari.math.u-bordeaux.fr/`.

Sorbonne Universités, UPMC Paris 6, UMR 7606, LIP6, 75005, Paris, France
E-mail address: `alexandre.gelin@lip6.fr`

École Polytechnique Fédérale de Lausanne, EPFL IC LACAL, Switzerland

École Polytechnique Fédérale de Lausanne, EPFL IC LACAL, Switzerland